

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-132032

(43)Date of publication of application : 09.05.2003

(51)Int.Cl.

G06F 15/00 A61B 5/117

G06F 3/033 H04L 9/32

(21)Application number : 2001-326916

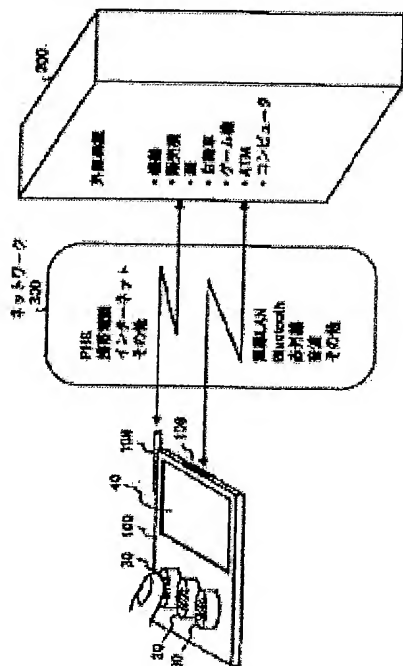
(71)Applicant : IKEDA MINORU

ID MOUSE JAPAN KK

(22)Date of filing : 24.10.2001

(72)Inventor : IKEDA MINORU

(54) PERSONAL AUTHENTICATION SYSTEM, AUTHENTICATION DEVICE, PERSONAL AUTHENTICATION METHOD, PROGRAM AND RECORDING MEDIUM



(57)Abstract:

PROBLEM TO BE SOLVED: To provide a system or the like that can recognize a fingerprint and sense the movement of a user's finger.

SOLUTION: An authentication device 100 has a recognition button 30 composed of an authentication chip that senses a user's fingerprint pattern and a switch button that senses the movement of the user's finger, a display device 40, a network 300 and a communication part 108 that communicates with the network 300 using a radio or wired communication means. The authentication device 100 recognizes whether or not the fingerprint pattern sensed with the authentication chip matches with the fingerprint pattern information of the user that has been previously registered, and recognizes whether or not the movement of the user's finger sensed with the switch button

and the recognition button 30 matches with the movement pattern information that has been previously registered.

Partial Translation of Document 4

Jpn. Pat. Appln. KOKAI Publication No. 2003-132032

Filing No.: 2001-326916

Filing Date: October 24, 2001

Applicant: IKEDA MINORU

ID MOUSE JAPAN KK

Priority: Not Claimed

KOKAI Date: May 9, 2003

Request for Examination: Not filed

Int.Cl.: G06F 15/00

A61B 5/117

G06F 3/033

H04L 9/32

**[A]****Page 2, Left Column, Line 1 to 19**

[What is Claimed is:]

[Claim 1]

A personal authentication system comprising an authentication device that authenticates that the user is a valid user, and an external device used by the user, which are mutually connected through a network, wherein

the authentication device includes

fingerprint sensing means for sensing a fingerprint pattern of the user,

fingerprint recognizing means for recognizing whether or not the fingerprint pattern sensed by the fingerprint sensing means matches with fingerprint pattern information of the user registered in advance,

motion sensing means for sensing a motion of a finger of the user, and

motion recognizing means for recognizing whether the motion sensed by the motion sensing means matches with motion pattern information registered in advance.

[Claim 2]

The personal authentication system according to claim 1, wherein

the authentication device is provided with the fingerprint recognizing means on a contact surface for a finger of the user in the motion sensing means.

**[B]****Page 3, Right Column, Line 34 to Page 4, Left Column, Line 4**

[0008] According to this system, a fingerprint pattern of the user is sensed, whether the sensed fingerprint pattern matches with fingerprint pattern information of the user registered in advance is recognized, a motion of a user's finger is sensed, and whether the sensed motion matches with motion pattern information registered in advance is recognized. Accordingly, by combining user authentication based on a fingerprint and authentication based on a motion, a "false accept rate" of accepting other users by false recognition can be lowered and security can be improved. A command and the like to an external device and the like, which are used after authentication, can also be input at the same time.

[0010] According to this system, a fingerprint recognizing means is provided on a contact surface for a finger of the user in the motion sensing means. Accordingly, the user can carry out fingerprint authentication and input of a motion in an integral manner. Fingerprint authentication and operation of a finger with respect to a button are carried out continuously on the same button. Accordingly, the user can feel less inhibited as compared with a case of carrying out only fingerprint authentication independently from operation.

**[C]****Page 7, Left Column, Line 25 to 33**

[0061] A motion information database 106b is a command information storing means for storing command information corresponding to operation pattern information. FIG. 21 is a diagram showing an example of information stored in the operation information database 106b.

[0062] As shown in FIG. 21, information stored in the operation information database 106b includes a user ID for uniquely identifying a user, motion pattern information relating to a pattern of a motion of a finger of the user, information of a command to be executed, and the like, which are associated with each other.

**[D]****Page 8, Left Column, Line 31 to Right Column, Line 30**

[0079]

[Concept of Motion of User's Finger]

Next, description will be made on details of a concept of a motion of a user's finger with reference to FIGS. 4 and 5. FIGS. 4 and 5 are diagrams showing examples of concepts of motions of a user's finger of the present system in the present embodiment.

[0080] The switch button 20 or the recognition chip 10 can sense a motion of a finger of the user. Alternatively, by combining a mechanical and electrical switch, such as a display device, in place of the switch button 20, a motion and a tilt of a finger in a horizontal direction are recognized.

[0081] In the above manner, the user can input directions, such as up, down, left, and right, in addition to pressing down the switch in a vertical direction. The above operation substitutes for operation of moving a mouse.

[0082] The switch button 20 or the recognition chip 10 can sense a motion of a finger. By combining a mechanical and electrical switch in place of the switch button 20, touching and releasing of a finger with respect to a recognition surface can be recognized. The above substitutes for click and double-click carried out by using a mouse button.

[0083] In general, a password is expressed by characters and numbers. These can be replaced by a series of rolling operations of a user's finger on the recognition button 30. In the above manner, strong security that is equivalent to one achieved by fingerprint authentication added with a password made up of a series of operations of a finger can be ensured by using only a single recognition button.

[0084] A motion pattern (also referred to as a motion sequence) can be used not only for improving strength of security, but also for instructing operation associated with a direction to an external device. For example, a motion pattern can be used for gradually increasing or decreasing a set value of a target external device, showing a moving direction of a robot arm or the like, or the like.

[0085] A motion sequence the user inputs in the recognition button 30 may be associated with some specific function of an external device.

[0086] For example, in a motion pattern shown in FIG. 4, a motion sequence made up of an upward motion, four clicks, and a leftward motion is registered as a command for moving to a privilege mode described later. In order to achieve application of the above motion sequence, a motion sequence can be input by using a recognition button, can be stored in the storage section 106, and, when necessary, can be transmitted to the outside and stored.

[0087] In the present system, a motion sequence is used in addition to user authentication using a fingerprint. In this manner, a plurality of meanings and functions can be provided to one recognition button beyond a range of functions of an original recognition button. In this manner, even a single recognition button can enable setting and switching of a plurality of security levels, control of complicated equipment, or the like that is available only to a permitted person or the owner.

7-11-2

(A) (B) (C) (D) 0079~0087

Doc 4

対応なし、英抄

(19) 日本国特許庁 (J/P) (12) 公開特許公報 (A) (11) 特許出願公開番号  
特開2003-132032  
(P2003-132032A)  
(43) 公開日 平成15年5月9日 (2003.5.9)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード(参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 F 4 C 0 3 8
A 6 1 B 5/117		3/033	3 1 0 Y 5 B 0 8 5
G 0 6 F 3/033	3 1 0	H 0 4 L 9/00	6 7 3 D 5 B 0 8 7
H 0 4 L 9/32		A 6 1 B 5/10	3 2 2 5 J 1 0 4

審査請求 未請求 請求項の数21 O L (全 21 頁)

(21) 出願番号	特願2001-326916(P2001-326916)	(71) 出願人	501125998 池田 実 千葉県船橋市習志野台2-21-4
(22) 出願日	平成13年10月24日 (2001.10.24)	(71) 出願人	501414478 アイディマウスジャパン株式会社 東京都中央区銀座2-14-12 東銀座ビル 4 F Q B 内
		(72) 発明者	池田 実 千葉県船橋市習志野台2-21-4
		(74) 代理人	100089118 弁理士 酒井 宏明 (外1名)

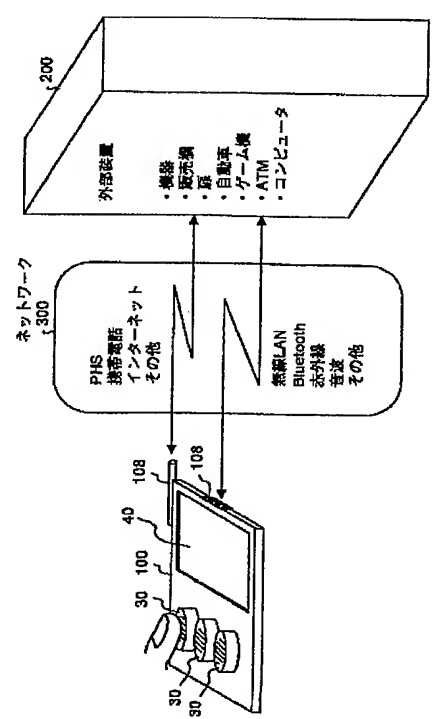
最終頁に続く

(54) 【発明の名称】 個人認証システム、認証装置、個人認証方法、プログラム、および、記録媒体

(57) 【要約】

【課題】 指紋の認識と利用者の指の動作を感知することのできるシステム等を提供することを課題とする。

【解決手段】 認証装置100は、利用者の指紋パターンを感知する認識チップと利用者の指の動作を感知するスイッチボタンとから構成される認識ボタン30と、ディスプレイ装置40と、ネットワーク300と各種の無線または有線の通信手段を用いて通信を行う通信部108とを備え、認識チップにて感知した指紋パターンが予め登録された利用者の指紋パターン情報と一致するか認識し、スイッチボタンと認識ボタン30にて感知した利用者の指の動作が予め登録された動作パターン情報と一致するか認識する。



A

## 【特許請求の範囲】

【請求項1】 利用者が正当な利用者であることを認証する認証装置と、上記利用者が使用する外部装置とをネットワークを介して相互に接続して構成された個人認証システムであって、  
上記認証装置は、  
利用者の指紋パターンを感知する指紋感知手段と、  
前記指紋感知手段にて感知した上記指紋パターンが予め登録された上記利用者の指紋パターン情報と一致するか認識する指紋認識手段と、  
利用者の指の動作を感知する動作感知手段と、  
前記動作感知手段にて感知した上記動作が予め登録された動作パターン情報と一致するか認識する動作認識手段と、  
を備えたことを特徴とする個人認証システム。

【請求項2】 上記認証装置は、  
上記動作感知手段における利用者の指の接触面上に上記指紋認識手段を設けたことを特徴とする請求項1に記載の個人認証システム。

【請求項3】 上記認証装置は、  
上記利用者の上記動作パターン情報に対応する命令情報を格納する命令情報格納手段と、  
上記動作認識手段により認識された前記動作パターン情報に対応する前記命令情報を検索する命令情報検索手段と、  
をさらに備えたことを特徴とする請求項1または2に記載の個人認証システム。

【請求項4】 上記認証装置は、  
上記命令情報検索手段にて検索された上記命令情報を実行する命令情報実行手段、  
をさらに備えたことを特徴とする請求項3に記載の個人認証システム。

【請求項5】 上記認証装置は、  
上記命令情報検索手段にて検索された上記命令情報を上記外部装置に送信する命令情報送信手段、  
をさらに備えたことを特徴とする請求項3または4に記載の個人認証システム。

【請求項6】 利用者の指紋パターンを感知する指紋感知手段と、  
前記指紋感知手段にて感知した上記指紋パターンが予め登録された上記利用者の指紋パターン情報と一致するか認識する指紋認識手段と、  
利用者の指の動作を感知する動作感知手段と、  
前記動作感知手段にて感知した上記動作が予め登録された動作パターン情報と一致するか認識する動作認識手段と、  
を備えたことを特徴とする認証装置。

【請求項7】 上記動作感知手段における利用者の指の接触面上に上記指紋認識手段を設けたことを特徴とする請求項6に記載の認証装置。

【請求項8】 上記利用者の上記動作パターン情報に対応する命令情報を格納する命令情報格納手段と、  
上記動作認識手段により認識された前記動作パターン情報に対応する前記命令情報を検索する命令情報検索手段と、  
をさらに備えたことを特徴とする請求項6または7に記載の認証装置。

【請求項9】 上記命令情報検索手段にて検索された上記命令情報を実行する命令情報実行手段と、  
をさらに備えたことを特徴とする請求項8に記載の認証装置。

【請求項10】 上記命令情報検索手段にて検索された上記命令情報を上記外部装置に送信する命令情報送信手段と、  
をさらに備えたことを特徴とする請求項8または9に記載の認証装置。

【請求項11】 利用者が正当な利用者であることを認証する認証装置と、  
上記利用者が使用する外部装置とをネットワークを介して相互に接続して構成された個人認証システムを用いて実行される個人認証方法であって、  
利用者の指紋パターンを感知する指紋感知ステップと、  
前記指紋感知ステップにて感知した上記指紋パターンが予め登録された上記利用者の指紋パターン情報と一致するか認識する指紋認識ステップと、  
利用者の指の動作を感知する動作感知ステップと、  
前記動作感知ステップにて感知した上記動作が予め登録された動作パターン情報と一致するか認識する動作認識ステップと、  
を含むことを特徴とする個人認証方法。

【請求項12】 上記動作感知ステップにおける利用者の指の接触面上に上記指紋認識ステップを設けたことを特徴とする請求項11に記載の個人認証方法。

【請求項13】 上記利用者の上記動作パターン情報に対応する命令情報を格納する命令情報格納ステップと、  
上記動作認識ステップにより認識された前記動作パターン情報に対応する前記命令情報を検索する命令情報検索ステップと、  
をさらに含むことを特徴とする請求項11または12に記載の個人認証方法。

【請求項14】 上記命令情報検索ステップにて検索された上記命令情報を実行する命令情報実行ステップ、  
をさらに含むことを特徴とする請求項13に記載の個人認証方法。

【請求項15】 上記命令情報検索ステップにて検索された上記命令情報を上記外部装置に送信する命令情報送信ステップ、  
をさらに含むことを特徴とする請求項13または14に記載の個人認証方法。

【請求項16】 利用者の指紋パターンを感知する指紋

感知ステップと、

前記指紋感知ステップにて感知した上記指紋パターンが予め登録された上記利用者の指紋パターン情報と一致するか認識する指紋認識ステップと、

利用者の指の動作を感知する動作感知ステップと、前記動作感知ステップにて感知した上記動作が予め登録された動作パターン情報と一致するか認識する動作認識ステップと、

を含むことを特徴とする、認証装置により実行される個人認証方法をコンピュータに実行させるためのプログラム。

【請求項17】 上記動作感知ステップにおける利用者の指の接触面に上記指紋認識ステップを設けたことを特徴とする請求項16に記載のプログラム。

【請求項18】 上記利用者の上記動作パターン情報に対応する命令情報を格納する命令情報格納ステップと、上記動作認識ステップにより認識された前記動作パターン情報に対応する前記命令情報を検索する命令情報検索ステップと、

をさらに含むことを特徴とする請求項16または17に記載のプログラム。

【請求項19】 上記命令情報検索ステップにて検索された上記命令情報を実行する命令情報実行ステップと、をさらに含むことを特徴とする請求項18に記載のプログラム。

【請求項20】 上記命令情報検索ステップにて検索された上記命令情報を上記外部装置に送信する命令情報送信ステップと、

をさらに含むことを特徴とする請求項18または19に記載のプログラム。

【請求項21】 請求項16から20に記載のプログラムを記録したことを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、利用者の指紋パターンを用いる個人認証システム、認証装置、個人認証方法、プログラム、および、記録媒体に関し、特に、利用者の指紋パターンと指の動作パターンとを感知する個人認証システム、認証装置、個人認証方法、プログラム、および、記録媒体に関する。

【0002】

【従来の技術】従来より、人間の指の指紋を認識することにより本人認証を行うことができる認証装置が存在する。現在市販されている指紋認識デバイスは、1秒あたり8回の指紋認証が可能のため連続的な本人確認が可能で、当該デバイスから指を離す、あるいは途中で他人に代わると直ちにそれを感知できるものがある。

【0003】

【発明が解決しようとする課題】しかしながら、従来の指紋認識デバイスでは利用者の指紋パターンのみで認識

を行っているので、万が一類似性の高い指紋を有する他人が利用者になりすまして利用することを完全に防止することができないという問題点を有していた。

【0004】また、従来の指紋認識デバイスでは、人間の指の動きを感知することができないため、認識後の装置のオペレーション動作等については、別途ボタン等を操作する必要があった。また、利用者は一度指紋認証をパスするとその後は認証動作をしなくて操作できるため、他人が真正の本人になりすまして操作することを排除できなかった。

【0005】このように、従来の認識装置等は数々の問題点を有しており、その結果、認識装置の利用者および管理者のいずれにとっても、利便性が悪く、また、利用効率が悪いものであった。

【0006】本発明は上記問題点に鑑みてなされたもので、指紋の認識と利用者の指の動作を感知することのできる、個人認証システム、認証装置、個人認証方法、プログラム、および、記録媒体を提供することを目的としている。

【0007】

【課題を解決するための手段】このような目的を達成するため、請求項1に記載の個人認証システムは、利用者が正当な利用者であることを認証する認証装置と、上記利用者が使用する外部装置とをネットワークを介して相互に接続して構成された個人認証システムであって、上記認証装置は、利用者の指紋パターンを感知する指紋感知手段と、前記指紋感知手段にて感知した上記指紋パターンが予め登録された上記利用者の指紋パターン情報と一致するか認識する指紋認識手段と、利用者の指の動作を感知する動作感知手段と、前記動作感知手段にて感知した上記動作が予め登録された動作パターン情報と一致するか認識する動作認識手段とを備えたことを特徴とする。

【0008】このシステムによれば、利用者の指紋パターンを感知し、感知した指紋パターンが予め登録された利用者の指紋パターン情報と一致するか認識し、利用者の指の動作を感知し、感知した動作が予め登録された動作パターン情報と一致するか認識するので、指紋による本人認証と動作による認証とを併用することにより他人を誤認して受け入れる「他人受け入れ率」を下げ、セキュリティを高めることができるようになり、また、認証後に使用する外部装置等への命令等を同時に入力することができるようになる。

【0009】また、請求項2に記載の個人認証システムは、請求項1に記載の個人認証システムにおいて、上記認証装置は、上記動作感知手段における利用者の指の接触面に上記指紋認識手段を設けたことを特徴とする。

【0010】このシステムによれば、動作感知手段における利用者の指の接触面に指紋認識手段を設けたので、利用者は指紋認証と動作の入力とを一体的におこなうこ



とができるようになる。また、指紋認証とボタンに対する指の操作を同一のボタン上で連続的に行うため、指紋認証だけを操作と独立して行う場合に比べ、心理的な抵抗を和らげることができる。

【0011】また、請求項3に記載の個人認証システムは、請求項1または2に記載の個人認証システムにおいて、上記認証装置は、上記利用者の上記動作パターン情報に対応する命令情報を格納する命令情報格納手段と、上記動作認識手段により認識された前記動作パターン情報に対応する前記命令情報を検索する命令情報検索手段とをさらに備えたことを特徴とする。

【0012】このシステムによれば、認証装置は、利用者の動作パターン情報に対応する命令情報を格納し、認識された動作パターン情報に対応する命令情報を検索するので、本人認証後の外部装置の操作等を一連の動作にて指定することができるようになる。また、指紋認証とボタンに対する指の操作を同一のボタン上で連続的に行うため、指紋認証だけを操作と独立して行う場合に比べ、心理的な抵抗を和らげることができる。

【0013】また、請求項4に記載の個人認証システムは、請求項3に記載の個人認証システムにおいて、上記認証装置は、上記命令情報検索手段にて検索された上記命令情報を実行する命令情報実行手段をさらに備えたことを特徴とする。

【0014】このシステムによれば、認証装置は、検索された命令情報を実行するので、特権モードからユーザモードへの移行などの各種の命令情報を指定した認識ボタン上の指の動作により実行することができるようになる。

【0015】また、請求項5に記載の個人認証システムは、請求項3または4に記載の認証装置において、上記認証装置は、上記命令情報検索手段にて検索された上記命令情報を上記外部装置に送信する命令情報送信手段をさらに備えたことを特徴とする。

【0016】このシステムによれば、認証装置は、検索された命令情報を外部装置に送信するので、外部装置に対する各種の命令情報を指定した動作により送信することができるようになる。

【0017】また、本発明は認証装置に関するものであり、請求項6に記載の認証装置は、利用者の指紋パターンを感知する指紋感知手段と、前記指紋感知手段にて感知した上記指紋パターンが予め登録された上記利用者の指紋パターン情報と一致するか認識する指紋認識手段と、利用者の指の動作を感知する動作感知手段と、前記動作感知手段にて感知した上記動作が予め登録された動作パターン情報と一致するか認識する動作認識手段とを備えたことを特徴とする。

【0018】この認証装置によれば、利用者の指紋パターンを感知し、感知した指紋パターンが予め登録された利用者の指紋パターン情報と一致するか認識し、利用者

の指の動作を感知し、感知した動作が予め登録された動作パターン情報と一致するか認識するので、指紋による本人認証と動作による認証とを併用することにより他人を誤認して受け入れる「他人受け入れ率」を下げ、セキュリティを高めることができるようになり、また、認証後に使用する外部装置等への命令等を同時に入力することができるようになる。

【0019】また、請求項7に記載の認証装置は、請求項6に記載の認証装置において、上記動作感知手段における利用者の指の接触面に上記指紋認識手段を設けたことを特徴とする。

【0020】この認証装置によれば、動作感知手段における利用者の指の接触面に指紋認識手段を設けたので、利用者は指紋認証と動作の入力とを一体的におこなうことができるようになる。また、指紋認証とボタンに対する指の操作を同一のボタン上で連続的に行うため、指紋認証だけを操作と独立して行う場合に比べ、心理的な抵抗を和らげることができる。

【0021】また、請求項8に記載の認証装置は、請求項6または7に記載の認証装置において、上記利用者の上記動作パターン情報に対応する命令情報を格納する命令情報格納手段と、上記動作認識手段により認識された前記動作パターン情報に対応する前記命令情報を検索する命令情報検索手段とをさらに備えたことを特徴とする。

【0022】この認証装置によれば、認証装置は、利用者の動作パターン情報に対応する命令情報を格納し、認識された動作パターン情報に対応する命令情報を検索するので、本人認証後の外部装置の操作等を一連の動作にて指定することができるようになる。また、指紋認証とボタンに対する指の操作を同一のボタン上で連続的に行うため、指紋認証だけを操作と独立して行う場合に比べ、心理的な抵抗を和らげることができる。

【0023】また、請求項9に記載の認証装置は、請求項8に記載の認証装置において、上記命令情報検索手段にて検索された上記命令情報を実行する命令情報実行手段をさらに備えたことを特徴とする。

【0024】この認証装置によれば、認証装置は、検索された命令情報を実行するので、特権モードからユーザモードへの移行などの各種の命令情報を指定した認識ボタン上の指の動作により実行することができるようになる。

【0025】また、請求項10に記載の認証装置は、請求項8または9に記載の認証装置において、上記命令情報検索手段にて検索された上記命令情報を上記外部装置に送信する命令情報送信手段をさらに備えたことを特徴とする。

【0026】この認証装置によれば、認証装置は、検索された命令情報を外部装置に送信するので、外部装置に対する各種の命令情報を指定した動作により送信するこ



とができるようになる。

【0027】また、本発明は個人認証方法に関するものであり、請求項11に記載の個人認証方法は、利用者が正当な利用者であることを認証する認証装置と、上記利用者が使用する外部装置とをネットワークを介して相互に接続して構成された個人認証システムを用いて実行される個人認証方法であって、利用者の指紋パターンを感知する指紋感知ステップと、前記指紋感知ステップにて感知した上記指紋パターンが予め登録された上記利用者の指紋パターン情報と一致するか認識する指紋認識ステップと、利用者の指の動作を感知する動作感知ステップと、前記動作感知ステップにて感知した上記動作が予め登録された動作パターン情報と一致するか認識する動作認識ステップとを含むことを特徴とする。

【0028】この方法によれば、利用者の指紋パターンを感知し、感知した指紋パターンが予め登録された利用者の指紋パターン情報と一致するか認識し、利用者の指の動作を感知し、感知した動作が予め登録された動作パターン情報と一致するか認識するので、指紋による本人認証と動作による認証とを併用することにより他人を誤認して受け入れる「他人受け入れ率」を下げ、セキュリティを高めることができるようになり、また、認証後に使用する外部装置等への命令等を同時に入力することができるようになる。

【0029】また、請求項12に記載の個人認証方法は、請求項11に記載の個人認証方法において、上記認証装置は、上記動作感知ステップにおける利用者の指の接触面に上記指紋認識ステップを設けたことを特徴とする。

【0030】この方法によれば、動作感知ステップにおける利用者の指の接触面に指紋認識ステップを設けたので、利用者は指紋認証と動作の入力とを一体的におこなうことができるようになる。また、指紋認証とボタンに対する指の操作を同一のボタン上で連続的に行うため、指紋認証だけを操作と独立して行う場合に比べ、心理的な抵抗を和らげることができる。

【0031】また、請求項13に記載の個人認証方法は、請求項11または12に記載の個人認証方法において、上記認証装置は、上記利用者の上記動作パターン情報に対応する命令情報を格納する命令情報格納ステップと、上記動作認識ステップにより認識された前記動作パターン情報に対応する前記命令情報を検索する命令情報検索ステップとをさらに含むことを特徴とする。

【0032】この方法によれば、認証装置は、利用者の動作パターン情報に対応する命令情報を格納し、認識された動作パターン情報に対応する命令情報を検索するので、本人認証後の外部装置の操作等を一連の動作にて指定することができるようになる。また、指紋認証とボタンに対する指の操作を同一のボタン上で連続的に行うため、指紋認証だけを操作と独立して行う場合に比べ、心

理的な抵抗を和らげることができる。

【0033】また、請求項14に記載の個人認証方法は、請求項13に記載の個人認証方法において、上記認証装置は、上記命令情報検索ステップにて検索された上記命令情報を実行する命令情報実行ステップをさらに含むことを特徴とする。

【0034】この方法によれば、認証装置は、検索された命令情報を実行するので、特権モードからユーザモードへの移行などの各種の命令情報を指定した認識ボタン上の指の動作により実行することができるようになる。

【0035】また、請求項15に記載の個人認証方法は、請求項13または14に記載の個人認証方法において、上記認証装置は、上記命令情報検索ステップにて検索された上記命令情報を上記外部装置に送信する命令情報送信ステップをさらに含むことを特徴とする。

【0036】この方法によれば、認証装置は、検索された命令情報を外部装置に送信するので、外部装置に対する各種の命令情報を指定した動作により送信することができるようになる。

【0037】また、本発明はプログラムに関するものであり、請求項16に記載のプログラムは、利用者の指紋パターンを感知する指紋感知ステップと、前記指紋感知ステップにて感知した上記指紋パターンが予め登録された上記利用者の指紋パターン情報と一致するか認識する指紋認識ステップと、利用者の指の動作を感知する動作感知ステップと、前記動作感知ステップにて感知した上記動作が予め登録された動作パターン情報と一致するか認識する動作認識ステップとを含むことを特徴とする。

【0038】このプログラムによれば、利用者の指紋パターンを感知し、感知した指紋パターンが予め登録された利用者の指紋パターン情報と一致するか認識し、利用者の指の動作を感知し、感知した動作が予め登録された動作パターン情報と一致するか認識するので、指紋による本人認証と動作による認証とを併用することにより他人を誤認して受け入れる「他人受け入れ率」を下げ、セキュリティを高めることができるようになり、また、認証後に使用する外部装置等への命令等を同時に入力することができるようになる。

【0039】また、請求項17に記載のプログラムは、請求項16に記載のプログラムにおいて、上記動作感知ステップにおける利用者の指の接触面に上記指紋認識ステップを設けたことを特徴とする。

【0040】このプログラムによれば、動作感知ステップにおける利用者の指の接触面に指紋認識ステップを設けたので、利用者は指紋認証と動作の入力とを一体的におこなうことができるようになる。また、指紋認証とボタンに対する指の操作を同一のボタン上で連続的に行うため、指紋認証だけを操作と独立して行う場合に比べ、心理的な抵抗を和らげることができる。

【0041】また、請求項18に記載のプログラムは、

請求項16または17に記載のプログラムにおいて、上記利用者の上記動作パターン情報に対応する命令情報を格納する命令情報格納ステップと、上記動作認識ステップにより認識された前記動作パターン情報に対応する前記命令情報を検索する命令情報検索ステップとをさらに含むことを特徴とする。

【0042】このプログラムによれば、利用者の動作パターン情報に対応する命令情報を格納し、認識された動作パターン情報に対応する命令情報を検索するので、本人認証後の外部装置の操作等を一連の動作にて指定することができるようになる。また、指紋認証とボタンに対する指の操作を同一のボタン上で連続的に行うため、指紋認証だけを操作と独立して行う場合に比べ、心理的な抵抗を和らげることができる。

【0043】また、請求項19に記載のプログラムは、請求項18に記載のプログラムにおいて、上記命令情報検索ステップにて検索された上記命令情報を実行する命令情報実行ステップをさらに含むことを特徴とする。

【0044】このプログラムによれば、検索された命令情報を実行するので、特権モードからユーザモードへの移行などの各種の命令情報を指定した認識ボタン上の指の動作により実行することができるようになる。

【0045】また、請求項20に記載のプログラムは、請求項18または19に記載のプログラムにおいて、上記命令情報検索ステップにて検索された上記命令情報を上記外部装置に送信する命令情報送信ステップをさらに含むことを特徴とする。

【0046】このプログラムによれば、検索された命令情報を外部装置に送信するので、外部装置に対する各種の命令情報を指定した動作により送信することができるようになる。

【0047】また、本発明は記録媒体に関するものであり、請求項21に記載の記録媒体は、上記請求項16から20のいずれか一つに記載されたプログラムをコンピュータに実行させるためのプログラムを記録したことを特徴とする。

【0048】この記録媒体によれば、当該記録媒体に記録されたプログラムをコンピュータに読み取らせて実行することによって、請求項16から20のいずれか一つに記載されたプログラムをコンピュータを利用して実現することができ、これら各プログラムと同様の効果を得ることができる。

【0049】

【発明の実施の形態】以下に、本発明にかかる個人認証システム、認証装置、個人認証方法、プログラム、および、記録媒体の実施の形態を図面に基づいて詳細に説明する。なお、この実施の形態によりこの発明が限定されるものではない。

【0050】〔本システムの概要〕以下、本システムの概要について説明し、その後、本システムの構成および

処理等について詳細に説明する。図1は本システムの全体構成の一例を示すブロック図であり、該システム構成のうち本発明に係る部分のみを概念的に示している。

【0051】本システムは、利用者が正当な利用者であることを認証する認証装置100と、上記利用者が使用する外部装置200とをネットワーク300を介して相互に接続して構成されている。

【0052】このシステムは、概略的に、以下の基本的特徴を有する。すなわち、認証装置100は、利用者の指紋パターンを感知する認識チップ10と利用者の指の動作を感知する認識ボタン30と、ディスプレイ装置40と、ネットワーク300と各種の無線または有線の通信手段を用いて通信を行う通信部108とを備え、認識チップ10にて感知した指紋パターンが予め登録された利用者の指紋パターン情報と一致するか認識し、認識ボタン30にて感知した利用者の指の動作が予め登録された動作パターン情報と一致するか認識する。

【0053】ここで、認識ボタン30は、スイッチボタン20における利用者の指の接触面に認識チップ10を設けている場合を一例に説明する。

【0054】また、認証装置100は、利用者の指の動作パターン情報に対応する命令情報を格納し、認識ボタン30により認識された動作パターン情報に対応する命令情報を検索し、検索された命令情報を実行し、また、検索された命令情報を通信部108を介して外部装置200に送信する。

【0055】〔システム構成〕以下、このような基本的特徴を具現化するための、本システムの構成について説明する。

【0056】〔システム構成—認証装置100〕まず、認証装置100の構成について説明する。図2は、本発明が適用される認証装置100の構成の一例を示すブロック図であり、該構成のうち本発明に係る部分のみを概念的に示している。図2において認証装置100は、概略的に、利用者の指紋パターンを感知する認識チップ10、利用者の指の動作を感知するスイッチボタン20、利用者の指の動作を感知するディスプレイ装置などのディスプレイ装置40、認証装置100の全体を統括的に制御するCPU等の制御部102、通信回線等に接続されるルータ等の通信装置（図示せず）に接続される通信制御インターフェース部104、各種のデータベース（認証情報データベース106a～動作情報データベース106b）を格納する記憶部106、外部装置と各種の無線または有線の通信手段を用いて通信を行う通信部108、および、入出力装置に接続される入出力制御インターフェース部110を備えて構成されており、これら各部は任意の通信路を介して通信可能に接続されている。さらに、この認証装置100は、ルータ等の通信装置および専用線等の有線または無線の通信回線を介

して、ネットワーク300に通信可能に接続されている。

【0057】記憶部106に格納される各種のデータベース（認証情報データベース106a～動作情報データベース106b）は、固定ディスク装置等のストレージ手段であり、各種処理やウェブサイト提供に用いる各種のプログラムやテーブルやファイルやデータベースやウェブページ用ファイル等を格納する。

【0058】これら記憶部106の各構成要素のうち、認証情報データベース106aは、利用者の指紋に関する認証情報を格納する認証情報格納手段である。図20は、認証情報データベース106aに格納される認証情報の一例を示す図である。

【0059】この認証情報データベース106aに格納される情報は、図20に示すように、各利用者を一意に識別するための利用者ID、各利用者の指紋パターン情報などを相互に関連付けて構成されている。

【0060】ここで、指紋パターン情報は、例えば、指紋の画像データや、その画像データについて動的計画法（DP法）や隠れマルコフモデル（HMM）や遺伝的アルゴリズム（GA）などの既存のパターン解析技術を用いて解析して抽出した指紋の特徴に関する情報などである。また、指紋パターン情報には、画像データ、テキストファイル、動画ファイル等が含まれてもよい。

【0061】また、動作情報データベース106bは、動作パターン情報に対応する命令情報を格納する命令情報格納手段である。図21は、動作情報データベース106bに格納される情報の一例を示す図である。

【0062】この動作情報データベース106bに格納される情報は、図21に示すように、利用者を一意に識別するための利用者ID、利用者の指の動作のパターンに関する動作パターン情報、実行される命令情報等を相互に関連付けて構成されている。

【0063】ここで、動作パターン情報は、例えば、動作パターンの座標データや、その座標データについて動的計画法（DP法）や隠れマルコフモデル（HMM）や遺伝的アルゴリズム（GA）などの既存のパターン解析技術を用いて解析して抽出した指の動作の特徴に関する情報などである。また、動作パターン情報には、画像データ、テキストファイル、動画ファイル等が含まれてもよい。

【0064】また、図2において、通信制御インターフェース部104は、認証装置100とネットワーク300（またはルータ等の通信装置）との間における通信制御を行う。すなわち、通信制御インターフェース部104は、他の端末と通信回線を介してデータを通信する機能を有する。

【0065】また、図2において、通信部108は、認識ボタン30、ディスプレイ装置40、他の入力装置や出力装置の制御を行う。ここで、出力装置としては、モ

ニタ（家庭用テレビを含む）の他、スピーカを用いることができる（なお、以下においては出力装置をモニタとして記載する）。また、入力装置としては、キーボード、マウス、および、マイク等を用いることができる。また、モニタも、マウスと協働してポインティングデバイス機能を実現する。

【0066】また、図2において、制御部102は、OS（Operating System）等の制御プログラム、各種の処理手順等を規定したプログラム、および所要データを格納するための内部メモリを有し、これらのプログラム等により、種々の処理を実行するための情報処理を行う。制御部102は、機能概念的に、認識アルゴリズム部102a、命令情報実行部102b、および、動作モード管理部102cを備えて構成されている。

【0067】このうち、認識アルゴリズム部102aは、指紋感知手段にて感知した指紋パターンが予め登録された利用者の指紋パターン情報と一致するか認識する指紋認識手段であり、また、動作感知手段にて感知した動作が予め登録された動作パターン情報と一致するか認識する動作認識手段である。

【0068】認識アルゴリズム部102aは、例えば、動的計画法（DP法）や隠れマルコフモデル（HMM）や遺伝的アルゴリズム（GA）などの既存のパターン解析技術を用いて感知した指紋パターンや動作パターンを解析して特徴を抽出し、その特徴を認証情報データベース106aに予め登録された指紋パターン情報や、動作情報データベース106bに予め登録された動作パターン情報と比較して、指紋や動作を認識する。

【0069】また、命令情報実行部102bは、動作認識手段により認識された動作パターン情報に対応する前記命令情報を検索する命令情報検索手段であり、また、命令情報検索手段にて検索された命令情報を実行する命令情報実行手段である。

【0070】また、動作モード管理部102cは、認証装置100の各種の動作モードを管理する動作モード管理手段である。なお、これら各部によって行なわれる処理の詳細については、後述する。

【0071】〔システム構成—ネットワーク300〕次に、ネットワーク300の構成について説明する。ネットワーク300は、認証装置100と外部装置200とを相互に接続する機能を有し、例えば、無線LANやBluetoothや光通信ネットワークや公衆電話網やインターネット等である。

【0072】〔システムの処理〕次に、このように構成された本実施の形態における本システムの処理の一例について、以下に図3～図19を参照して詳細に説明する。

【0073】〔認識ボタン30の概念〕まず、認識ボタン30の概念について図3を参照して説明する。図3

は、本実施形態における本システムの認識ボタン30の概念を示す概念図である。

【0074】認識チップ10は、例えば、1秒あたり8回の指紋認証が可能のため連続的な本人確認が可能であり、デバイスから指を離す、あるいは途中で他人に代わると直ちにそれを感知できるものを使用しても良い。

【0075】スイッチボタン20は、指の移動をセンスできる。左右と前後への指の傾き（ローリング）を本デバイスが感知し、それを画面上のカーソルの動きに連動させポインティングデバイスとしても利用できる。また、図3に示すように、スイッチボタン20と認識チップ10とを認識ボタン30として一体的に構成すると、例えば、カーソルの移動中も本人自身が操作していることを保証できるようになる。

【0076】ただし、上記機能が他の代替手段で実現されていてもよい。例えば、スイッチボタン20のポインティング機能は、ボタン状のスイッチの外縁に配置したマイクロスイッチあるいは圧電素子などのセンサーを使って実現されていても本発明の有効性は保たれ、スイッチボタン20の実現方式とは無関係に成立する。

【0077】スイッチボタン20における利用者の指の接触面に認識チップ10を設けたので、本人でなければボタンが押せない（反応しない）、あるいは押しても対象物が動作しない認証装置を実現することができる。また、ボタンを押した人間が特定できる認証装置を実現することができる。

【0078】また、スイッチボタン20は機械的に押下できるものだけでなく、位置や形状の変化を伴わずに指紋の認識と押下を検知するもの（例えば感圧センサなど）も含む。

【0079】[利用者の指の動作の概念] 次に、利用者の指の動作の概念の詳細について図4および図5を参照して説明する。図4および図5は、本実施形態における本システムの利用者の指の動作の概念の一例を示す図である。

【0080】スイッチボタン20または認識チップ10によって、利用者の指の動きを感知することができる。あるいは、スイッチボタン20の代わりにディスプレイ装置等の機械的・電気的なスイッチを併用することによって指の水平方向の動きや傾きを認識する。

【0081】これによって、利用者がスイッチを垂直方向に押下する以外に、上、下、左、右などの方向の入力ができる。これは、机上でマウスを移動する動作を代替するものである。

【0082】また、スイッチボタン20または認識チップ10によって、指の動きを感知することができる。スイッチボタン20の代わりに機械的・電気的なスイッチを併用することによって指の認識面へのタッチとデタッチを認識することができる。これは、マウスボタンを用いるクリック、ダブルクリックを代替する。

【0083】また、一般的にパスワードは文字や数字で表すが、認識ボタン30上の一連の利用者の指のローリング操作でそれを代替することができる。これにより、単一の認識ボタンのみでも指紋認証に加えて一連の指の動作からなるパスワードを付加したのと同様な強固なセキュリティを確保できる。

【0084】また、動作パターン（モーションシーケンスとも呼ぶ）はセキュリティの強度を上げるだけでなく、方向に関係付けた操作を外部装置に指示するためにも利用できる。例えば、対象の外部装置の設定値を段階的に上げたり、下げたり、あるいはロボットアームなどの動作方向を示したりするなどの用途がある。

【0085】また、利用者が認識ボタン30に入力したモーションシーケンスは、外部装置の何らかの特定の機能に結びつけられるようにしてもよい。

【0086】例えば、図4に示す動作パターンでは、上方向、クリック4回、左方向のモーションシーケンスを後述する特権モード移行のコマンドとして登録している。こうしたモーションシーケンスの応用を実現するために、モーションシーケンスを認識ボタンから入力できると共に、記憶部106に記憶させることができ、かつ必要であれば外部に送信して保存できる。

【0087】本システムでは、指紋による本人認証に加えてモーションシーケンスを用いることによって、本来の認識ボタンの機能範囲を超えて、1つの認識ボタンに複数の意味や機能をもたせることが可能になる。これにより、単独の認識ボタンであっても、許された人あるいは本人だけが利用できる、複数のセキュリティレベルの設定や切り替え、あるいは複雑な機器の制御などが可能になる。

【0088】[動作モードの管理] 次に、動作モードの管理の詳細について図6および図7を参照して説明する。図6は、本実施形態における本システムの動作モードの移行の一例を示す図である。

【0089】本装置による一般ユーザが利用する際の指紋の認証機能には、常に認証を行う認証モードと、認証を行わない非認証モードがあり、それを特権モードの操作で切り替えられるようにする。

【0090】認証モードでは認識ボタン30は常に上に置かれた、あるいは押下した指の指紋を読み取り、予め登録された本人の指紋であるか否かを識別する。一方、非認証モードでは、認識ボタンは指紋の認証を行わず、常に本人であると解釈する。認証モードの切り替えは、いったん特権モードに移行してから行う。

【0091】また、この認証装置100には特権モードとユーザモードがあり、それぞれのモードでは以下の機能が実行できる。

【0092】まず、特権モードでは、新規に真正な指紋を登録したり、これまでの登録済み指紋を抹消したり、モーションシーケンスを登録したりすることができる。

また、特権モードから認証ユーザモードへ移行したり、あるいは非認証モードへ移行したりすることができる。

【0093】次に、認証ユーザモードでは、特権モードから認証ユーザモードに移行できたり、全ての、あるいはアプリケーションが指示した、ユーザモードの操作に対して指紋認証を行ったりすることができる。

【0094】次に、非認証ユーザモードでは、特権モードから非認証ユーザモードに移行できたり、全てのユーザモードにおける操作が認証なしで自由に操作したりすることができる。

【0095】ここで、「操作」とは、各種のボタンの押下、指のローリング、クリック、メニュー選択、ペン入力などの操作で利用者が行うことができるあらゆる物を指す。

【0096】また、図7は、本実施形態における本システムの動作モードの移行処理の一例を示すフローチャートである。

【0097】ユーザモードから特権モードへの移行は、予めユーザが定めたモーションシーケンスを入力することによって行う。従ってデバイスは、利用者の指のアクションを常に監視して、モーションメモリの内容と照合し、一致した場合に特権モードに移行する。

【0098】まず、初期設定を行う特権モードになる(ステップSA-1)。

【0099】次に、特権モードで許される操作等を実行する(ステップSA-2)。

【0100】次に、ボタンあるいはメニューからモーションシーケンス登録を選択し、一連の指の動作を入力する(ステップSA-3)。

【0101】次に、フィンガーアクション(移行のコマンド)をモーションメモリである動作情報データベース106bに登録する(ステップSA-4)。

【0102】次に、ユーザモードへの移行を選択するためのボタンを押下あるいは移動メニューを選択する(ステップSA-5)。

【0103】ユーザモードへ移行すると、ユーザモードの操作(ステップSA-7)を行い、またフィンガーアクション監視によりモーションメモリと照合を行い、モーションメモリ内容と指の動作が一致する場合には(ステップSA-8)、特権モードへ移行し(ステップSA-10)、また、モーションメモリ内容と指の動作が不一致の場合には(ステップSA-9)、ユーザモードを続行する(ステップSA-6)。

【0104】〔複数の認識ボタンを設置〕次に、複数の認識ボタンを設置の詳細について図8を参照して説明する。図8は、本実施形態における本システムの複数の認識ボタンを設置の一例を示す図である。

【0105】本実施形態においては、認証装置100は、複数の認識ボタン30を組み合わせた。各認識ボタン30は、数字や文字あるいは、あるいはYes、No

や「承認」などの意味に対応付けられる。複数の認識ボタンを選択的に押下することによって、より複雑な情報の入力や利用者の意思の表現を可能とする。

【0106】それら複数のボタンの少なくとも1つのボタンの押下は特定の人にしかできない、あるいは押しても動作しない状態にすることができる。また、ボタンを押下した人が特定できるようになる。これにより入力した情報内容とその発信者の本人性が証明できる。

【0107】〔認識ボタンを操作対象物に設置〕次に、認識ボタンを操作対象物に設置する場合の詳細について図9～図11を参照して説明する。図9～図11は、本実施形態における本システムの認識ボタンを操作対象物に設置する場合の一例を示す図である。

【0108】図9に示すように、1つまたは複数の認識ボタンを操作盤上に配置する。その操作盤を動作を制限したい対象物に取り付け、許された人間に対してのみ選択的な操作を許す。

【0109】例としては、閉錠・開錠(家屋、倉庫、車、その他薬品、危険物保管庫等)、コンピュータの起動や、アプリケーションの起動、機器の操作、薬品や危険物の管理庫、金融機関のATMその他などがあるが、これ以外の全ての用途を制約しない。

【0110】次に図10に示すように、認識ボタンを操作対象物に設置する場合の基本構成を示す。外部装置におけるデータベースなどの実装方式はいかなるものであってもよい。

【0111】門扉や販売機や装置などに取り付けられた認識ボタンからは、認証結果あるいはモーションシーケンスから生成されたPIN(Personal Identification Number)が生成される。PINは必ずしもPINそのものとは限らず、時刻などと組合せて暗号化した仮想PINや一度しか利用できないワンタイムパスワードであっても良い。

【0112】一方、装置側にはコンピュータやデータベースが装備され、予め受け入れを認める指紋に対応するPINをデータベースに保存しておく。指紋認識ボタンによる認識結果によって生成されたPINとデータベース中のPINが照合装置で照合され、合致すれば要求の受け入れとなり、一致するものが無い場合は拒否となる。

【0113】次に図11に示すように、認識ボタンを操作対象物に設置する場合の別の構成を示す。本人が持参する携帯電話、カードなどの携帯可能な機器に別の認識装置を用いて予め本人のPINを書き込んでおく。

【0114】装置側に設置された認識ボタンを押したりモーションを入力すると、認識結果としてPINを発生する。一方、認識ボタンを設置した装置からカードや携帯電話に対してPIN読み出しの信号が送られる。カードや携帯電話から暗号化されたPINが装置に対して送出される。



【0115】装置側では先に認識結果として認識ボタンが生成したPINと、外部から受け取ったPINを照合し、カードや携帯電話の持参人が本人である認証を行う。両者が一致すれば受け入れ、不一致であれば拒否となる。

【0116】〔表示装置等との連動〕次に、表示装置との連動の詳細について図12を参照して説明する。図12は、本実施形態における本システムの認識ボタンと表示装置との連動の一例を示す図である。

【0117】認識ボタン30は、ボタン上の指の傾き変化を認識、あるいは周囲に配したボタンの押下によって方向を指示できる。それをディスプレイ装置40などの表示装置上のカーソル移動と連動させることが可能である。すなわち、カーソル移動を認識ボタン上の指の傾き変化で行うことができる。また、機器やアプリケーション側から利用者個人が特定できるので、個人向けに特殊化した情報やサービスを提供する高度なパーソナライズ機能が実現できる。

【0118】また、カーソル移動中も指紋認識が可能なので、カーソルの移動を選択的に制限でき、本人に許された機能メニューに対する移動のみにカーソルの動きを限定できる。すなわち、アクセスを制限されたメニューは選択できない。

【0119】メニューの選択は認識ボタン上でクリック(ボタンに指を素早く一回タッチ、あるいは2回タッチ)することにより行う。クリックによるメニュー選択は特定の許された利用者のみができる。これにより、クリック操作を行った利用者が特定できる。

【0120】外部装置としては、主に、コンピュータ、携帯電話、PDA、ゲーム機、業務用モバイル機器、キャッシュレジスタ、自動販売機などであるが、それらに限定されるものではない。

【0121】また、ディスプレイ装置あるいはスタイラスペンをポインティングデバイスとして利用する場合においても、認識ボタンは連続的に本人認証を繰り返すことによって、本人自身がポインティングデバイス进行操作していることを保証できる。

【0122】その場合は、一方の手で携帯機器を保持しながら指で認識ボタンを押さえることによって本人認証を行い、他方の手で画面へタッチしたりスタイラスペンをういて入力したりメニュー選択を行う。また、バーコードリーダなどでも類似の構成によって、本人認証とバーコードのスキニングが可能となる。

【0123】〔遠隔操作装置に実装した場合〕次に、本実施形態における本認証装置を遠隔操作装置に実装した場合の詳細について図13から図15を参照して説明する。図13から図15は、本実施形態における本認証装置を遠隔操作装置に実装した場合の一例を示す図である。

【0124】図13に示すように、テレビや空調のリモ

ートコントロールボックス用の機器あるいは携帯電話機またはPDAなどの携帯情報機器などに認証装置100を設置する。これにより特定の人にしかメニューなどの画面操作ができない、あるいは操作した人が特定できる携帯可能な遠隔操作装置が成立する。これにより、本人が本人用の遠隔操作装置を所持する場合のみ、対象物に対して操作を指示できる。

【0125】本装置を所持する本人は、本人に許された動作、例えば、閉錠・開錠、車のエンジンの始動・停止、コンピュータの起動など、本人を認証し、操作内容を本人の権限内に限定でき、かつその範囲内において、あらゆる種類の遠隔操作が可能となる。

【0126】この遠隔操作には機器等を操作すること以外に自動販売機からの購入やチケット購入などに必要な操作も含む。装置は小型化によってカード状の形状とすることも可能である。

【0127】また図14に示すように、この遠隔操作装置は、有線、無線、赤外線などを通じて操作対象の機器とコミュニケーションして、操作者の意志を外部装置に反映することができる。

【0128】本操作機器と対象機器のインターフェースを統一することにより複数の対象を操作できる汎用の遠隔操作装置になる。

【0129】これは、所持者からみると真正の本人であることを証明する万能キーのような役割を果たし、認証装置100を備えた遠隔操作装置さえもっていれば、アクセスが許されているいかなる対象に対しても所有者の意思を送り出すことができる。

【0130】これはいわば所有者と利用者が同一であることを常に保証する電子印鑑付きのリモコンのようなもので、これとインターフェースが取れる機器であれば、本人からの指示であることを保証される。ここで用いる通信手段は十分に安全で秘匿性が高い手段を選択する。

【0131】また、必要であれば、両者間で交換されるメッセージに電子署名などを含めることによってより、完全な認証にすることもできる。

【0132】また、図15に示すように、万能キーとして機能する本認証装置を備えた遠隔操作装置は様々な媒体に組み込むことが可能であり、例えば、カード、PDA、携帯電話などに組み込むことができる。

【0133】〔本認証装置を個人特定センサーとして実現する場合〕次に、本認証装置を個人特定センサーとして実現する場合の詳細について図16を参照して説明する。図16は、本実施形態における本システムの本認証装置を個人特定センサーとして実現する場合の一例を示す図である。

【0134】万能キーとして機能する本認証装置を備えた遠隔操作装置からの信号を受け取る側を中心にして見ると、その対象に対して興味を持っている人が、対象に向けて万能キーを押下することは、対象物に対してその

人が興味を持っていることを表している。

【0135】従って、万能キーの受信装置（個人特定センサー）をポスター、ショウウィンドウやマネキンに付けたタグなど様々な場所や対象に設置することによって、興味を持つ人間を特定できる人間センサーとして利用できる。

【0136】図16は、個人特定センサーを用いた個人顧客に対する特別な情報や催し物などを伝える応用例を示す図である。

【0137】携帯型の万能キーを持ちセンサーが設置された対象に向かって認識ボタンを押下する。

【0138】すると、個人を示すIDなどが、万能キーから個人特定センサーに送られる。これにより誰が、どこにある、何に、いつ、興味を示したかが把握できる。

【0139】さらに、個人特定センサーからID情報などを顧客管理システムに送り、購入履歴などでランキングされた特別価格や優待情報など、特定顧客向けの特別な情報を万能キーに返すことができる。

【0140】また、万能キーの所有者は表示画面などを通じてその内容を知ることができる。これにより、特定個人を対象とする個別的なマーケティングやセールス活動が可能になる。

【0141】さらに、双方向的な通信を利用して、商品やサービスに対して複数の万能キー所有者が値を付け、その中の最高価格で落札するオークションなども可能である。本発明の範囲は、提示の例に限定されず他の応用例に対しても適用されるものである。

【0142】〔本認証装置を他の外部装置と連携する場合〕次に、本認証装置を他の外部装置と連携する場合の詳細について図17および図18を参照して説明する。図17および図18は、本実施形態における本システムの本認証装置を他の外部装置と連携する場合の一例を示す図である。

【0143】万能キーとして機能する本認証装置を備えた遠隔操作装置は、それ自体単独で構成されてもかまわないが、携帯電話やPDAなどの無線接続が可能なモバイル機器と一体化することができる（図17参照）。それによって機器が持つ通信機能と連動させ、遠隔対象との情報交換も可能とする。遠隔対象には電話回線の延長上に接続されたインターネットサービスの利用も含む。

【0144】これにより、目の前にある販売機など対象物に対する操作と、広域的な情報を管理しているネット系の情報システムを連携することが可能となる。

【0145】対象物は本人確認の信号を受けて動作するだけでなく、キャッシュレジスタのような機器が、通信によって口座番号やカード情報や電話番号などを受け取って、リアルタイムに決済を実行するような構成も可能である。また、安全確実に商品の購入代金やサービスの利用料金を本人の電話利用料金の請求に含めることもできる。

【0146】また、先のオークションのような応用では、個人特定センサーが設置されたポスター、掲示板あるいは、ショウウィンドウなどを介して公開された販売条件に対して、複数の購入希望者が、それぞれの万能キーを使って価格などの購入条件を個人特定センサーに対して提示するオークションの実現も可能である。

【0147】図18は、認証装置100と他の装置との連携の一例を示す模式図である。図18に示す構成は、本人性を保証する中継装置が近傍にある装置と電話回線とインターネットの先につながるコンピュータアプリケーションを連携させる構成とも言える。

【0148】〔本認証装置をハードキーとして実現する場合〕次に、本認証装置をハードキーとして実現する場合の詳細について図19を参照して説明する。図19は、本実施形態における本システムの本認証装置をハードキーとして実現する場合の一例を示す図である。

【0149】現在本人を認証するハードキーが各種開発されている。そのようなハードキーは、コンピュータのUSB（Universal Serial Bus）ポートや携帯電話の下部に挿入でき、ハードキーが挿入されていると本人が利用しているとみなし、コンピュータへログインでき暗号化された通信文から平文への復号などが行われる。

【0150】また携帯電話ではUIM（Universal Identity Module）が実用化されている。UIMには暗号化された電話番号、利用者IDなどが収められ、電話機などの本体に挿入すると所有者本人が利用しているものとみなし、所定の電話番号で利用できるようになる。また、UIMは電話機本体から取り外すことができ、別の電話機に取り付けることができる。

【0151】このようなハードキーは、本人が所有し利用している限りでは問題ないが、紛失したり、盗難、貸与などによって他人が利用できてしまう。つまり、ハードキーやUIMだけでは、他人のなりすましを防ぐことができない。

【0152】図19に示すように、ハードウェアキーに認証装置100を付加することにより、本人以外がハードキーを利用する危険を排除することができる。これにより、携帯機器の安全性が増し、企業における高額の取引や決済などが安全にできるようになる。

【0153】また、上述した機器、PDA、携帯電話、情報家電機器、カードあるいはハードキーなどは自由に組み合わせることが可能で、その場合でも認識ボタン30を用いた認証装置100の有効性は変わらない。

【0154】現行のハードキーは物理的に挿入できるソケットとして実装されているが、無線、赤外線など無線的な通信手段で実現されていてもよい。

【0155】また同様に、認識ボタンを携帯電話、レジスタやコンピュータあるいは自動車など装置側に設置し

て、個人認識ハードウェア側から送出されるPINと装置に設置された認識ボタンから得られるPINとの照合を行う構成であってもよい。

【0156】[本認証装置をプリペイドカードやスマートカード等として実現する場合]次に、本認証装置をプリペイドカードやスマートカード等として実現する場合の詳細について説明する。

【0157】本発明の認証装置100を、プリペイドカードやスマートカードなど現金の代替となる財が蓄積できるカードに設置することによって、カードの利用者が所有者本人であることを特定できるようになる。

【0158】また、物品やサービスの購入時に、代金をカードから安全に引き落とすことができる。

【0159】また同様に、認証装置100はカード読取装置側に設置して、カード側から送出されるPINと読取装置に設置した認識ボタンから得られるPINとの照合を行う構成であってもよい。

【0160】また、カードは接触式、非接触式であるかは問わない。

【0161】[他の実施の形態]さて、これまで本発明の実施の形態について説明したが、本発明は、上述した実施の形態以外にも、上記特許請求の範囲に記載した技術的思想の範囲内において種々の異なる実施の形態にて実施されてよいものである。

【0162】また、実施形態において説明した各処理のうち、自動的に行なわれるものとして説明した処理の全部または一部を手動的に行うこともでき、あるいは、手動的に行なわれるものとして説明した処理の全部または一部を公知の方法で自動的に行うこともできる。

【0163】この他、上記文書中や図面中で示した処理手順、制御手順、具体的な名称、各種の登録データや検索条件等のパラメータを含む情報、画面例、データベース構成については、特記する場合を除いて任意に変更することができる。

【0164】また、認証装置100に関して、図示の各構成要素は機能概念的なものであり、必ずしも物理的に図示の如く構成されていることを要しない。例えば、認証装置100の各サーバが備える処理機能、特に制御部にて行なわれる各処理機能については、その全部または任意の一部を、CPU(Central Processing Unit)および当該CPUにて解釈実行されるプログラムにて実現することができ、あるいは、ワイヤードロジックによるハードウェアとして実現することも可能である。なお、プログラムは、後述する記録媒体に記録されており、必要に応じて認証装置100に機械的に読み取られる。

【0165】また、認証装置100は、さらなる構成要素として、マウス等の各種ポインティングデバイスやキーボードやイメージスキャナやデジタイザ等から成る入力装置(図示せず)、入力データのモニタに用いる表示

装置(図示せず)、システムクロックを発生させるクロック発生部(図示せず)、および、各種処理結果その他のデータを出力するプリンタ等の出力装置(図示せず)を備えてもよく、また、入力装置、表示装置および出力装置は、それぞれ入出力制御インターフェース部110を介して制御部102に接続されてもよい。

【0166】記憶部106に格納される各種のデータベース等(認証情報データベース106a~動作情報データベース106b)は、RAM、ROM等のメモリ装置、ハードディスク等の固定ディスク装置、フレキシブルディスク、光ディスク等のストレージ手段であり、各種処理やウェブサイト提供に用いる各種のプログラムやテーブルやファイルやデータベースやウェブページ用ファイル等を格納する。

【0167】また、認証装置100は、既知のパーソナルコンピュータ、ワークステーション等の情報処理端末等の情報処理装置にプリンタやモニタやイメージスキャナ等の周辺装置を接続し、該情報処理装置に本発明の方法を実現させるソフトウェア(プログラム、データ等を含む)を実装することにより実現してもよい。

【0168】さらに、認証装置100の分散・統合の具体的な形態は図示のものに限られず、その全部または一部を、各種の負荷等に応じた任意の単位で、機能的または物理的に分散・統合して構成することができる。例えば、各データベースを独立したデータベース装置として独立に構成してもよく、また、処理の一部をCGI(Common Gateway Interface)を用いて実現してもよい。

【0169】また、本発明にかかるプログラムを、コンピュータ読み取り可能な記録媒体に格納することもできる。ここで、この「記録媒体」とは、フロッピー(R)ディスク、光磁気ディスク、ROM、EPROM、EEPROM、CD-ROM、MO、DVD等の任意の「可搬用の物理媒体」や、各種コンピュータシステムに内蔵されるROM、RAM、HD等の任意の「固定用の物理媒体」、あるいは、LAN、WAN、インターネットに代表されるネットワークを介してプログラムを送信する場合の通信回線や搬送波のように、短期にプログラムを保持する「通信媒体」を含むものとする。

【0170】また、「プログラム」とは、任意の言語や記述方法にて記述されたデータ処理方法であり、ソースコードやバイナリコード等の形式を問わない。なお、「プログラム」は必ずしも単一的に構成されるものに限られず、複数のモジュールやライブラリとして分散構成されるものや、OS(Operating System)に代表される別個のプログラムと協働してその機能を達成するものをも含む。なお、実施の形態に示した各装置において記録媒体を読み取るための具体的な構成、読み取り手順、あるいは、読み取り後のインストール手順等については、周知の構成や手順を用いることができ



る。

【0171】また、ネットワーク300は、認証装置100と外部装置200とを相互に接続する機能を有し、例えば、インターネットや、イントラネットや、LAN（有線／無線の双方を含む）や、VANや、パソコン通信網や、公衆電話網（アナログ／デジタルの双方を含む）や、専用回線網（アナログ／デジタルの双方を含む）や、CATV網や、IMT2000方式、GSM方式またはPDC／PDC-P方式等の携帯回線交換網／携帯パケット交換網や、無線呼出網や、Bluetooth等の局所無線網や、PHS網や、CS、BSまたはISDB等の衛星通信網等のうちいずれかを含んでもよい。すなわち、本システムは、有線・無線を問わず任意のネットワークを介して、各種データを送受信することができる。

【0172】

【発明の効果】以上詳細に説明したように、本発明によれば、利用者の指紋パターンを感知し、感知した指紋パターンが予め登録された利用者の指紋パターン情報と一致するか認識し、利用者の指の動作を感知し、感知した動作が予め登録された動作パターン情報と一致するか認識するので、指紋による本人認証と動作による認証とを併用することにより他人を誤認して受け入れる「他人受け入れ率」を下げ、セキュリティを高めることができる個人認証システム、認証装置、個人認証方法、プログラム、および、記録媒体を提供することができる。

【0173】また、これにより、認証後に使用する外部装置等への命令等を同時に入力することができる個人認証システム、認証装置、個人認証方法、プログラム、および、記録媒体を提供することができる。

【0174】また、本発明によれば、動作感知手段における利用者の指の接触面に指紋認識手段を設けたので、利用者は指紋認証と動作の入力とを一体的におこなうことができる個人認証システム、認証装置、個人認証方法、プログラム、および、記録媒体を提供することができる。

【0175】また、本発明によれば、認証装置は、利用者の動作パターン情報に対応する命令情報を格納し、認識された動作パターン情報に対応する命令情報を検索するので、本人認証後の外部装置の操作等を一連の動作にて指定することができる個人認証システム、認証装置、個人認証方法、プログラム、および、記録媒体を提供することができる。

【0176】また、本発明によれば、認証装置は、検索された命令情報を実行するので、特権モードからユーザモードへの移行などの各種の命令情報を指定した認識ボタン上の指の動作により実行することができる個人認証システム、認証装置、個人認証方法、プログラム、および、記録媒体を提供することができる。

【0177】また、本発明によれば、認証装置は、検索

された命令情報を外部装置に送信するので、外部装置に対する各種の命令情報を指定した動作により送信することができる個人認証システム、認証装置、個人認証方法、プログラム、および、記録媒体を提供することができる。

【図面の簡単な説明】

【図1】本システムの全体構成の一例を示すブロック図である。

【図2】本発明が適用される認証装置100の構成の一例を示すブロック図である。

【図3】本実施形態における本システムの認識ボタン30の概念を示す概念図である。

【図4】本実施形態における本システムの利用者の指の動作の概念の一例を示す図である。

【図5】本実施形態における本システムの利用者の指の動作の概念の一例を示す図である。

【図6】本実施形態における本システムの動作モードの移行の一例を示す図である。

【図7】本実施形態における本システムの動作モードの移行処理の一例を示すフローチャートである。

【図8】本実施形態における本システムの複数の認識ボタンを設置の一例を示す図である。

【図9】本実施形態における本システムの認識ボタンを操作対象物に設置する場合の一例を示す図である。

【図10】本実施形態における本システムの認識ボタンを操作対象物に設置する場合の一例を示す図である。

【図11】本実施形態における本システムの認識ボタンを操作対象物に設置する場合の一例を示す図である。

【図12】本実施形態における本システムの認識ボタンと表示装置との連動の一例を示す図である。

【図13】本実施形態における本認証装置を遠隔操作装置に実装した場合の一例を示す図である。

【図14】本実施形態における本認証装置を遠隔操作装置に実装した場合の一例を示す図である。

【図15】本実施形態における本認証装置を遠隔操作装置に実装した場合の一例を示す図である。

【図16】本実施形態における本システムの本認証装置を個人特定センサーとして実現する場合の一例を示す図である。

【図17】本実施形態における本システムの本認証装置を他の外部装置と連携する場合の一例を示す図である。

【図18】本実施形態における本システムの本認証装置を他の外部装置と連携する場合の一例を示す図である。

【図19】本実施形態における本システムの本認証装置をハードキーとして実現する場合の一例を示す図である。

【図20】認証情報データベース106aに格納される認証情報の一例を示す図である。

【図21】動作情報データベース106bに格納される情報の一例を示す図である。

## 【符号の説明】

100 認証装置

10 認識チップ

20 スイッチボタン

30 認識ボタン

40 ディスプレイ装置

102 制御部

102a 認識アルゴリズム部

102b 命令情報実行部

102c 動作モード管理部

104 通信制御インターフェース部

106 記憶部

106a 認証情報データベース

106b 動作情報データベース

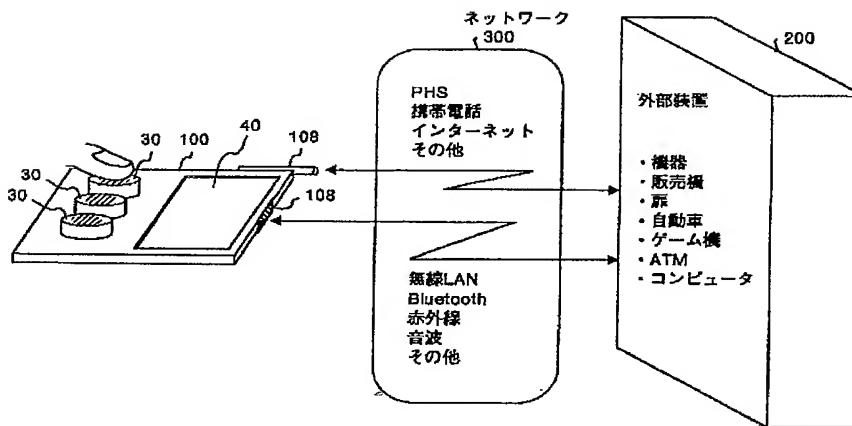
108 通信部

110 入出力制御インターフェース部

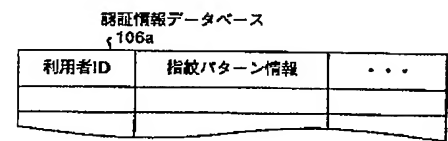
200 外部装置

300 ネットワーク

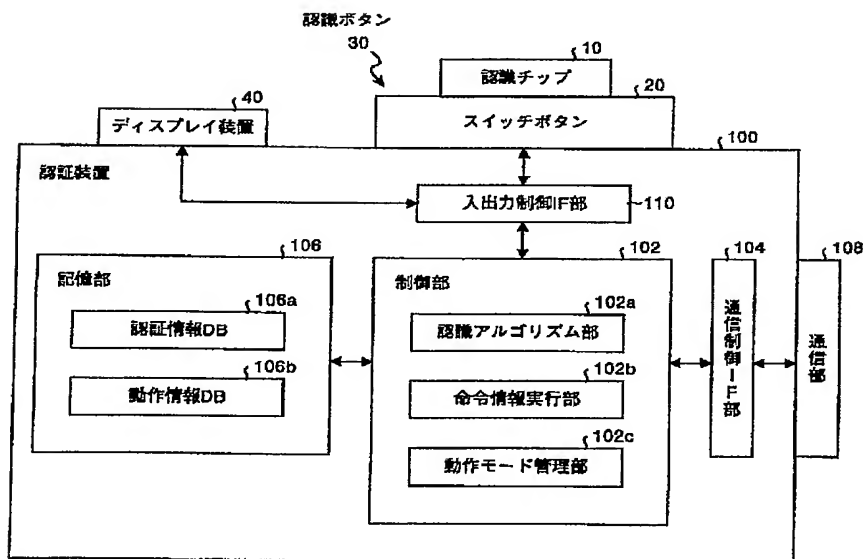
【図1】



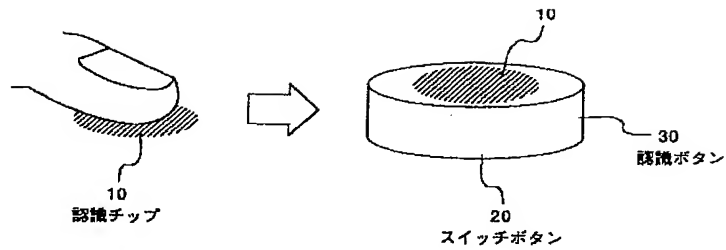
【図20】



【図2】



【図3】

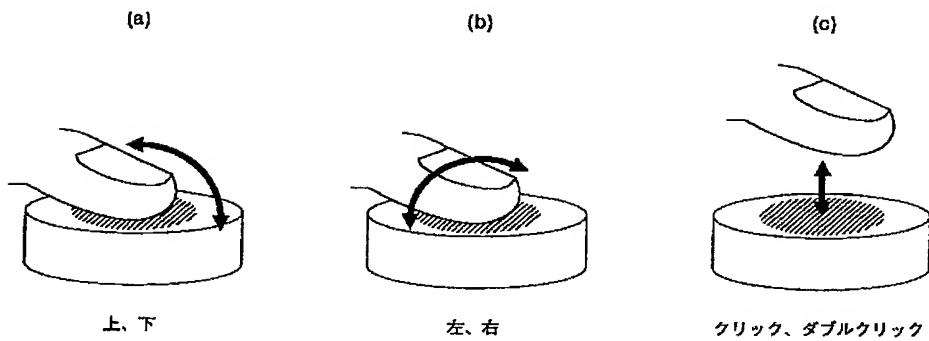


【図21】

動作情報データベース  
108b

利用者ID	動作パターン情報	命令情報	...

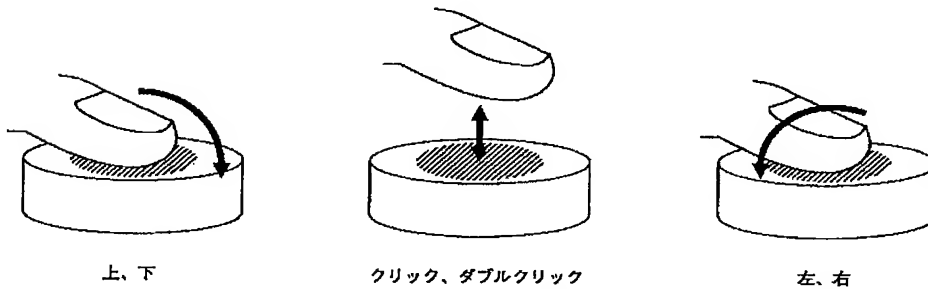
【図4】



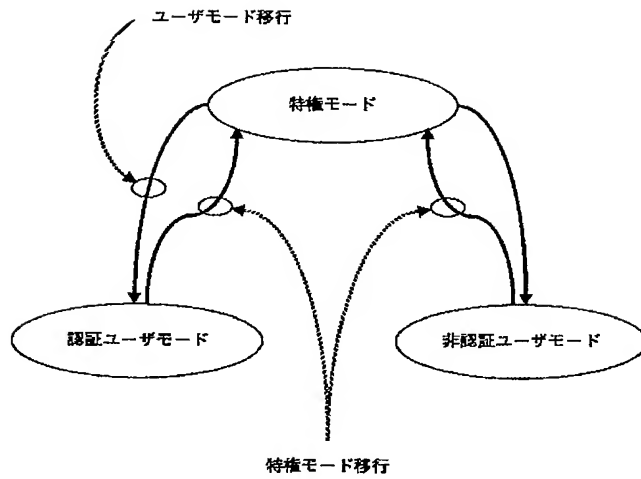
【図5】

例：〈上、4クリック、左〉の操作列で特権モードに移行する場合のモーションシーケンス

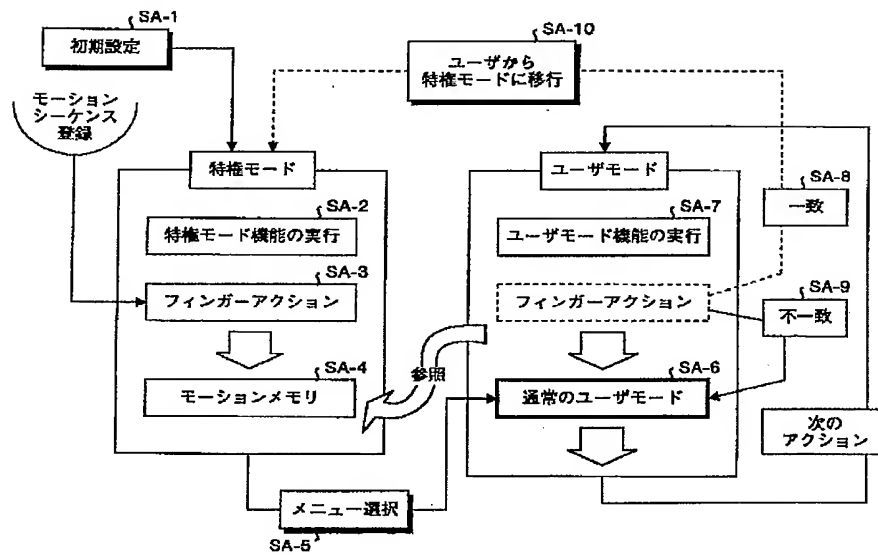
上 → 4回クリック → 左



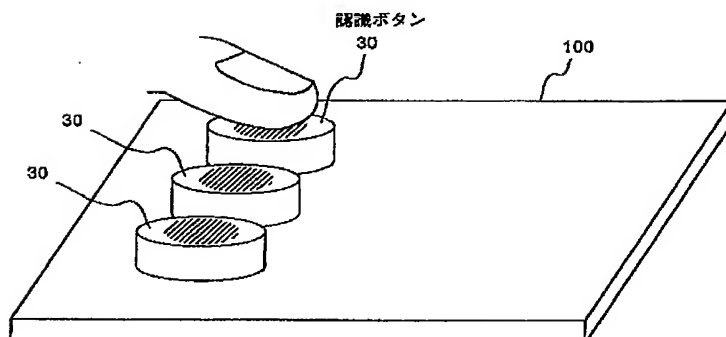
【図6】



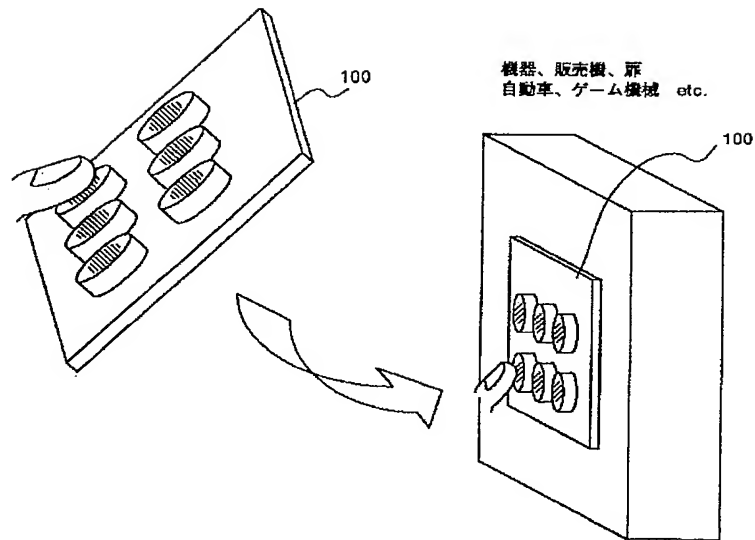
【図7】



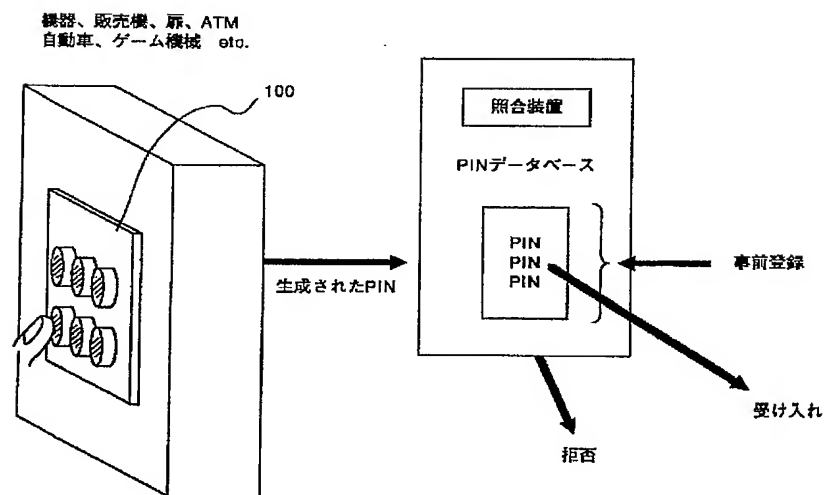
【図8】



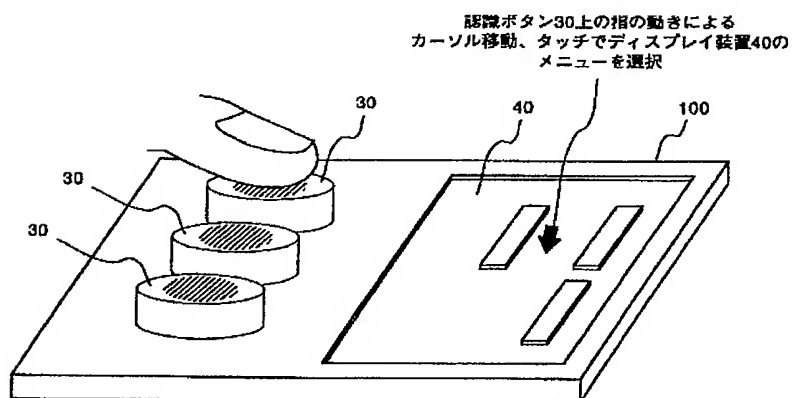
【図9】



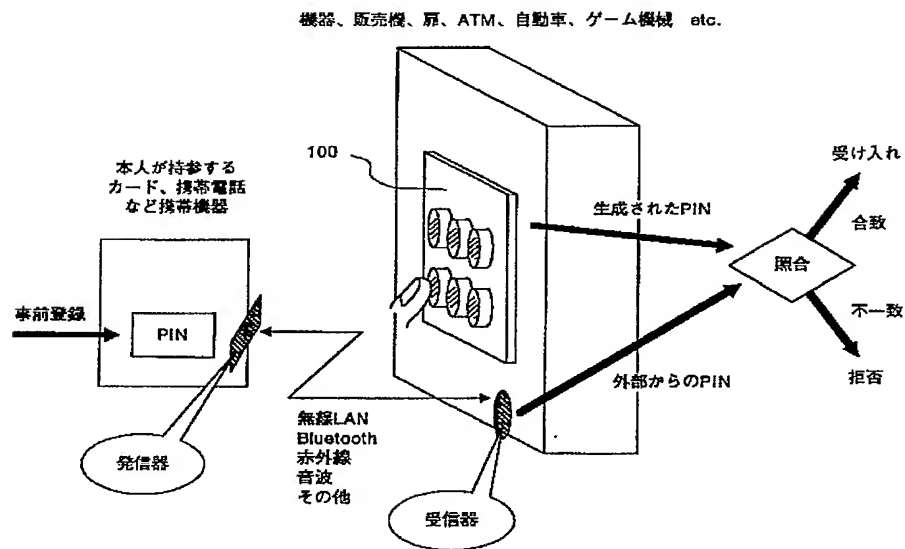
【図10】



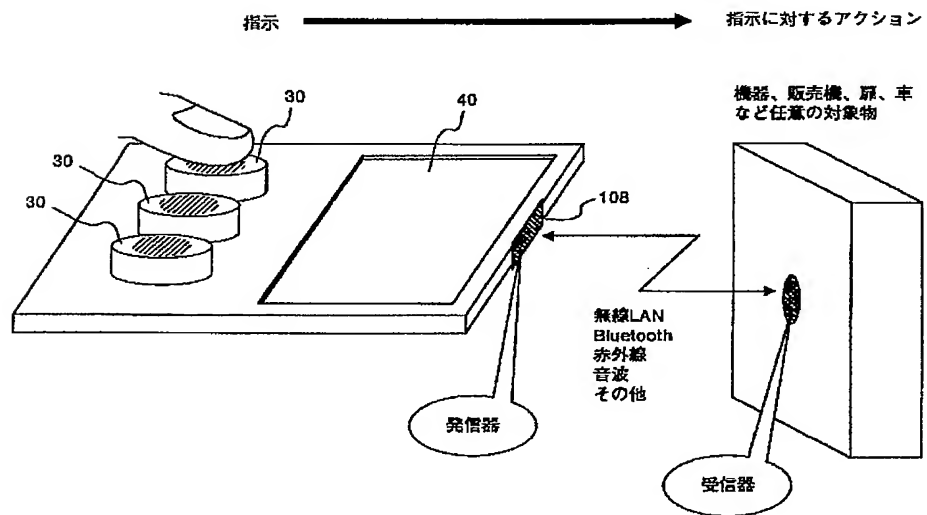
【図12】



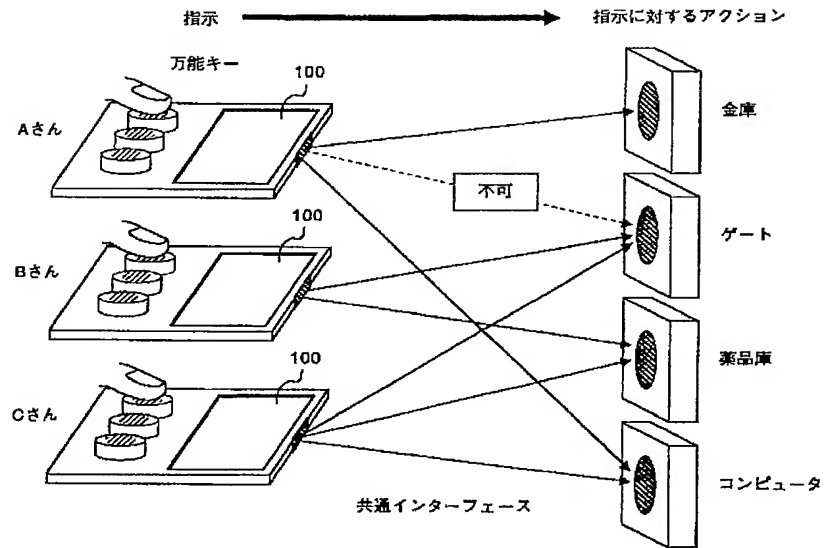
【図11】



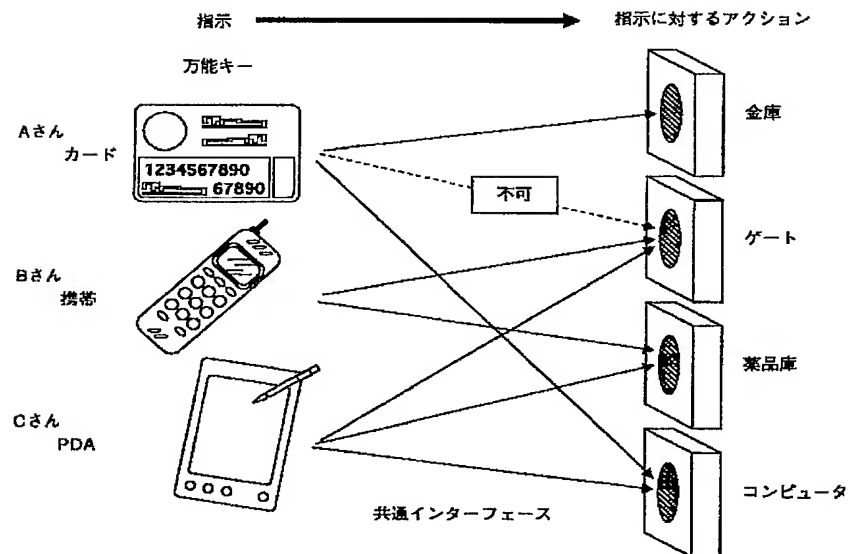
【図13】



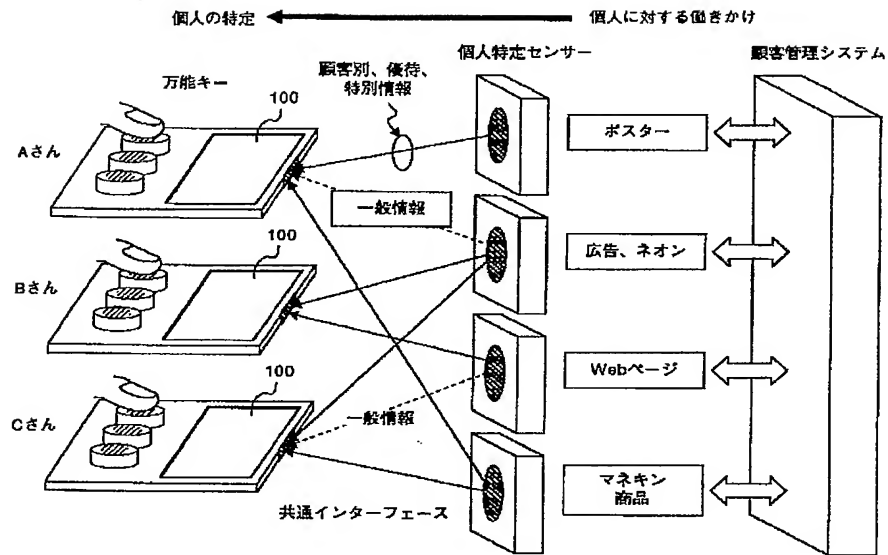
【図14】



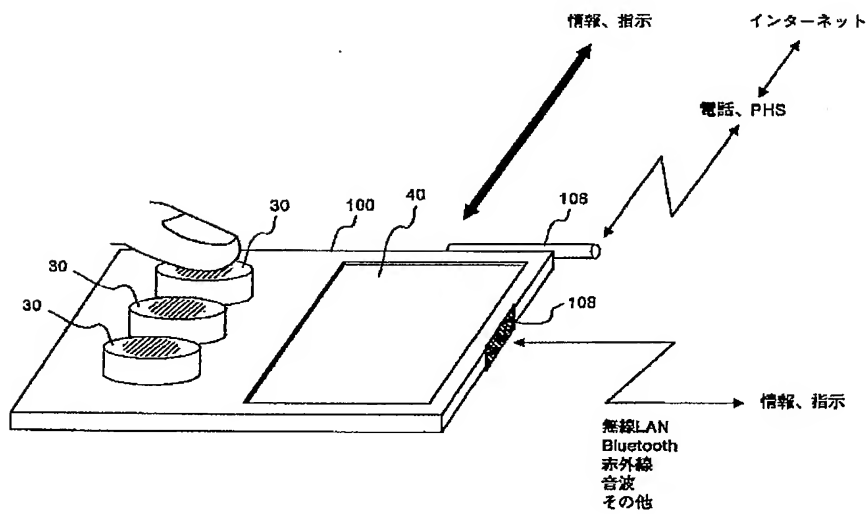
【図15】



【図16】

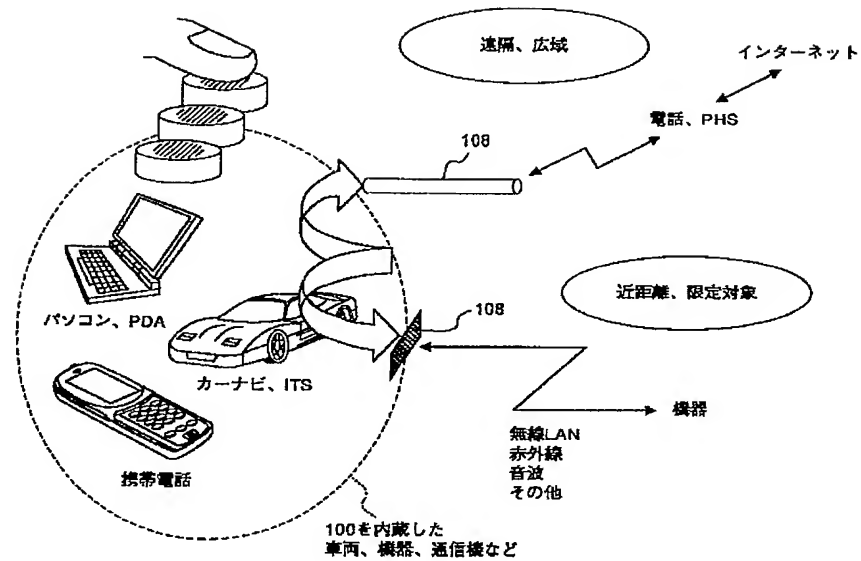


【図17】

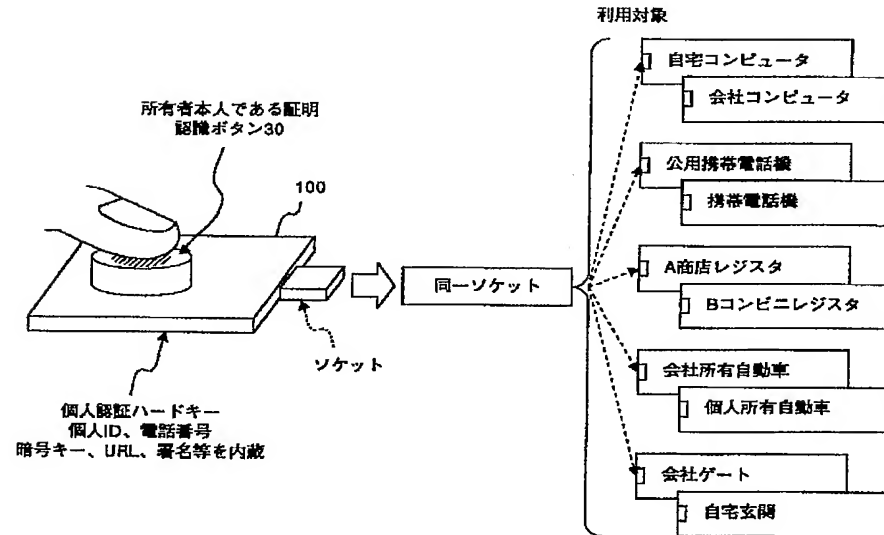




【図18】



【図19】



フロントページの続き

Fターム(参考) 4C038 FF01 FF05  
 5B085 AE25 AE26 BE01  
 5B087 AA02 BC11 BC16  
 5J104 AA07 KA01 KA17 PA07